In the Claims:

Please cancel claims 26, 54, and 62. Please amend claims 28, 30-31, 50-51, 55-59, and 63-67. The claims are as follows:

1-25. (Canceled)

26. (Canceled)

27. (Canceled)

28. (Currently amended) The method of claim ~~26~~ 51, wherein the at least one rule includes a data size for fingerprint authentication, a data size for voice print authentication, or a combination thereof.

29. (Canceled)

30. (Currently amended) The method of claim ~~26~~ 50, wherein said registering the authentication policy of the second server comprises registering the authentication policy of the second server in an authentication policy table of the first server, wherein the authentication policy table of the first server comprises an authentication policy of each server of the plurality of servers registered therein, and wherein the authentication policy table of the first server further comprises:

a server address of each server registered therein; and

a relative priority of each server of a group of servers having a same authentication policy in the authentication policy table.

31. (Currently amended) The method of claim ~~26~~ 50, wherein said registering the authentication policy of the second server comprises registering the authentication policy of the second server in an authentication policy table of the first server, wherein the authentication policy table of the first server comprises an authentication policy of each server of the plurality of servers registered therein, wherein the authentication policy of the second server is identical to an authentication policy of the first server, wherein a first common user identifier (ID) exists in an authentication information Lightweight Directory Access Protocol (LDAP) of the first server and in an authentication information LDAP of the second server, wherein the first common user ID is used by a first user in the first server and by a second user in the second server such that the second user differs from the first user, and wherein the method further comprises:

after said registering the authentication policy of the second server, registering by the first server the first common user ID in a exceptional ID table of the first server, wherein the exceptional ID table of the first server stores common user IDs and an indication of one or more servers associated with each common user ID stored in the exceptional ID table of the first server.

32-49. (Canceled)

50. (Currently amended) ~~The method of claim 26~~ A method for recording server authentication information, said method comprising:

establishing, by a first server of a plurality of servers in a federated computing environment, a trusting relationship between the first server and a second server of the plurality of servers, wherein said establishing the trusting relationship comprises exchanging, by the first server, an electronic certificate of the first server with an electronic certificate of the second server in accordance with a Public Key Infrastructure (PKI) method;

after said establishing the trusting relationship, obtaining by the first server an authentication policy of the second server, wherein an authentication policy for each server of the plurality of servers is defined as at least one rule of each server for authenticating users of the federated computing environment; and

after said obtaining the authentication policy of the second server, registering by the first server the authentication policy of the second server within the first server, wherein the at least one rule consists of four rules, said four rules consisting of a number of alphabetic characters of a user identification (ID), a number of numeric characters of the user ID, a data size for fingerprint authentication, and a data size for voice print authentication.

51. (Currently amended) ~~The method of claim 26~~ A method for recording server authentication information, said method comprising:

establishing, by a first server of a plurality of servers in a federated computing environment, a trusting relationship between the first server and a second server of the plurality of servers, wherein said establishing the trusting relationship comprises exchanging, by the first server, an electronic certificate of the first server with an electronic certificate of the second server in accordance with a Public Key Infrastructure (PKI) method;

after said establishing the trusting relationship, obtaining by the first server an authentication policy of the second server, wherein an authentication policy for each server of the plurality of servers is defined as at least one rule of each server for authenticating users of the federated computing environment; and

after said obtaining the authentication policy of the second server, registering by the first server the authentication policy of the second server within the first server,

wherein the method further comprises:

receiving, by the first server, an access request from a user to access the federated computing environment, wherein the first server comprises an authentication policy table that comprises the authentication policy of each server of the plurality of servers registered therein;

after said receiving the access request, receiving by the first server input authentication information from the user;

obtaining, by the first server, a server address of the second server, wherein the authentication policy of the second server matches an authentication policy of the first server;

transmitting, by the first server to the second server via the server address of the second server, the input authentication information;

after said transmitting the input authentication information to the second server, receiving by the first server from the second server a notification that the second server has successfully authorized the user; and

after said receiving the notification that the second server has successfully authorized the user, permitting the user to access the federated computing environment, wherein said permitting is performed by the first server.

52. (Previously presented) The method of claim 51, wherein after said transmitting the input authentication information to the second server and before said permitting the user to access the federated computing environment, the method further comprises:

receiving by the first server from the second server a token that may be used by the user to access the federated computing environment; and

sending, by the first server, the token to the user.

53. (Previously presented) The method of claim 52, wherein the token is a credential and a cookie.

54. (Canceled)

55. (Currently amended) The system of claim ~~54~~ 59, wherein the at least one rule includes a data size for fingerprint authentication, a data size for voice print authentication, or a combination thereof.

56. (Currently amended) The system of claim ~~54~~ 58, wherein said third program code for registering the authentication policy of the second server comprises code for registering the

authentication policy of the second server in an authentication policy table of the first server, wherein the authentication policy table of the first server comprises an authentication policy of each server of the plurality of servers registered therein, wherein the authentication policy table of the first server further comprises:

a server address of each server registered therein; and

a relative priority of each server of a group of servers having a same authentication policy in the authentication policy table.

57. (Currently amended) The system of claim ~~54~~ 58, wherein said third program code for registering the authentication policy of the second server comprises code for registering the authentication policy of the second server in an authentication policy table of the first server, wherein the authentication policy table of the first server comprises an authentication policy of each server of the plurality of servers registered therein, wherein the authentication policy of the second server is identical to an authentication policy of the first server, wherein a first common user identifier (ID) exists in an authentication information Lightweight Directory Access Protocol (LDAP) of the first server and in an authentication information LDAP of the second server, wherein the first common user ID is used by a first user in the first server and by a second user in the second server such that the second user differs from the first user, and wherein the system further comprises:

program code, stored on the computer readable storage medium, for registering by the first server the first common user ID in a exceptional ID table of the first server after said registering the authentication policy of the second server, wherein the exceptional ID table of the first server

stores common user IDs and an indication of one or more servers associated with each common user ID stored in the exceptional ID table of the first server.

58. (Currently amended) ~~The system of claim 54~~ A system for recording server authentication information, said system comprising:

a first server of a plurality of servers in a federated computing environment; and

a computer readable storage medium;

first program code for establishing, by the first server, a trusting relationship between the first server and a second server comprised by the plurality of servers, wherein said establishing the trusting relationship comprises exchanging, by the first server, an electronic certificate of the first server with an electronic certificate of the second server in accordance with a Public Key Infrastructure (PKI) method;

second program code for obtaining by the first server an authentication policy of the second server after said establishing the trusting relationship, wherein an authentication policy for each server of the plurality of servers is defined as at least one rule of each server for authenticating users of the federated computing environment; and

third program code for registering by the first server the authentication policy of the second server within the first server after said obtaining the authentication policy of the second server, wherein the first program code, the second program code, and the third program code are stored on the computer readable storage medium, and wherein the at least one rule consists of four rules, said four rules consisting of a number of alphabetic characters of a user identification

(ID), a number of numeric characters of the user ID, a data size for fingerprint authentication, and a data size for voice print authentication.

59. (Currently amended) ~~The system of claim 54~~ A system for recording server authentication information, said system comprising:

a first server of a plurality of servers in a federated computing environment; and

a computer readable storage medium;

first program code for establishing, by the first server, a trusting relationship between the first server and a second server comprised by the plurality of servers, wherein said establishing the trusting relationship comprises exchanging, by the first server, an electronic certificate of the first server with an electronic certificate of the second server in accordance with a Public Key Infrastructure (PKI) method;

second program code for obtaining by the first server an authentication policy of the second server after said establishing the trusting relationship, wherein an authentication policy for each server of the plurality of servers is defined as at least one rule of each server for authenticating users of the federated computing environment; and

third program code for registering by the first server the authentication policy of the second server within the first server after said obtaining the authentication policy of the second server,

wherein the first program code, the second program code, and the third program code are stored on the computer readable storage medium, and

wherein the system further comprises:

fourth program code for receiving, by the first server, an access request from a user to access the federated computing environment, wherein the first server comprises an authentication policy table that comprises the authentication policy of each server of the plurality of servers registered therein;

fifth program code for receiving by the first server input authentication information from the user after said receiving the access request;

sixth program code for obtaining, by the first server, a server address of the second server, wherein the authentication policy of the second server matches an authentication policy of the first server;

seventh program code for transmitting, by the first server to the second server via the server address of the second server, the input authentication information;

eighth program code for receiving by the first server from the second server a notification that the second server has successfully authorized the user after said transmitting the input authentication information to the second server; and

ninth program code for permitting the user to access the federated computing environment, wherein said permitting is performed by the first server after said receiving the notification that the second server has successfully authorized the user,

wherein the fourth program code, the fifth program code, the sixth program code, the seventh program code, the eighth program code, and the ninth program code are stored on the computer readable storage medium.

60. (Previously presented) The system of claim 59, wherein the system further comprises:

tenth program code for receiving by the first server from the second server a token that may be used by the user to access the federated computing environment after said transmitting the input authentication information to the second server and before said permitting the user to access the federated computing environment; and

eleventh program code for sending, by the first server, the token to the user ,

wherein the tenth program code and the eleventh program code are stored on the computer readable storage medium.

61. (Previously presented) The system of claim 60, wherein the token is a credential and a cookie.

62. (Canceled)

63. (Currently amended) The computer program product of claim ~~62~~ 67, wherein the at least one rule includes a data size for fingerprint authentication, a data size for voice print authentication, or a combination thereof.

64. (Currently amended) The computer program product of claim ~~62~~ 66, wherein said third program code for registering the authentication policy of the second server comprises code for registering the authentication policy of the second server in an authentication policy table of the first server, wherein the authentication policy table of the first server comprises an authentication policy of each server of the plurality of servers registered therein, wherein the authentication policy table of the first server further comprises:

a server address of each server registered therein; and

a relative priority of each server of a group of servers having a same authentication policy in the authentication policy table.

65. (Currently amended) The computer program product of claim ~~62~~ 66, wherein said third program code for registering the authentication policy of the second server comprises code for registering the authentication policy of the second server in an authentication policy table of the first server, wherein the authentication policy table of the first server comprises an authentication policy of each server of the plurality of servers registered therein, wherein the authentication policy of the second server is identical to an authentication policy of the first server, wherein a first common user identifier (ID) exists in an authentication information Lightweight Directory Access Protocol (LDAP) of the first server and in an authentication information LDAP of the second server, wherein the first common user ID is used by a first user in the first server and by a second user in the second server such that the second user differs from the first user, and wherein the computer program product further comprises:

program code, stored on the computer readable storage medium, for registering by the first server the first common user ID in a exceptional ID table of the first server after said registering the authentication policy of the second server, wherein the exceptional ID table of the first server stores common user IDs and an indication of one or more servers associated with each common user ID stored in the exceptional ID table of the first server.

66. (Currently amended) A computer program product for recording server authentication information, said computer program product comprising:

a computer readable storage medium;

first program code for establishing, by a first server of a plurality of servers, a trusting relationship between the first server and a second server comprised by the plurality of servers, wherein said establishing the trusting relationship comprises exchanging, by the first server, an electronic certificate of the first server with an electronic certificate of the second server in accordance with a Public Key Infrastructure (PKI) method;

second program code for obtaining by the first server an authentication policy of the second server after said establishing the trusting relationship, wherein an authentication policy for each server of the plurality of servers is defined as at least one rule of each server for authenticating users of the federated computing environment; and

third program code for registering by the first server the authentication policy of the second server within the first server after said obtaining the authentication policy of the second server,

wherein the first program code, the second program code, and the third program code are stored on the computer readable storage medium, and wherein the at least one rule consists of four rules, said four rules consisting of a number of alphabetic characters of a user identification (ID), a number of numeric characters of the user ID, a data size for fingerprint authentication, and a data size for voice print authentication.

67. (Currently amended) ~~The computer program product of claim 62~~ A computer program product for recording server authentication information, said computer program product comprising:

a computer readable storage medium;

first program code for establishing, by a first server of a plurality of servers, a trusting relationship between the first server and a second server comprised by the plurality of servers, wherein said establishing the trusting relationship comprises exchanging, by the first server, an electronic certificate of the first server with an electronic certificate of the second server in accordance with a Public Key Infrastructure (PKI) method;

second program code for obtaining by the first server an authentication policy of the second server after said establishing the trusting relationship, wherein an authentication policy for each server of the plurality of servers is defined as at least one rule of each server for authenticating users of the federated computing environment; and

third program code for registering by the first server the authentication policy of the second server within the first server after said obtaining the authentication policy of the second server,

wherein the first program code, the second program code, and the third program code are stored on the computer readable storage medium, and

wherein the computer program product further comprises:

fourth program code for receiving, by the first server, an access request from a user to access the federated computing environment, wherein the first server comprises an

authentication policy table that comprises the authentication policy of each server of the plurality of servers registered therein;

fifth program code for receiving by the first server input authentication information from the user after said receiving the access request;

sixth program code for obtaining, by the first server, a server address of the second server, wherein the authentication policy of the second server matches an authentication policy of the first server;

seventh program code for transmitting, by the first server to the second server via the server address of the second server, the input authentication information;

eighth program code for receiving by the first server from the second server a notification that the second server has successfully authorized the user after said transmitting the input authentication information to the second server; and

ninth program code for permitting the user to access the federated computing environment, wherein said permitting is performed by the first server after said receiving the notification that the second server has successfully authorized the user,

wherein the fourth program code, the fifth program code, the sixth program code, the seventh program code, the eighth program code, and the ninth program code are stored on the computer readable storage medium.

68. (Previously presented) The computer program product of claim 67, wherein the computer program product further comprises:

tenth program code for receiving by the first server from the second server a token that may be used by the user to access the federated computing environment after said transmitting the input authentication information to the second server and before said permitting the user to access the federated computing environment; and

eleventh program code for sending, by the first server, the token to the user ,

wherein the tenth program code and the eleventh program code are stored on the computer readable storage medium.

69. (Previously presented) The computer program product of claim 68, wherein the token is a credential and a cookie.